Snapcatch: Automatic Detection of Covert Timing Channels Using Image Processing and Machine Learning

Naveen Raj K[1], Parvez Mushraf M[2], Sheshan D B[3], Manikandan M[4]

BE, Department of CSE, Adhiyamaan College of Engineering, Hosur, India[1,2,3]

Assistant Professor, Department of CSE, Adhiyamaan College of Engineering, Hosur, India[4]

Abstract: **With the quick development of information exfiltration completed by digital assaults, Covert Timing Channels (CTC) have turned into a fast approaching organization security hazard that keeps on filling in both refinement and use. These sorts of channels use between appearance times to take delicate information from the designated networks. CTC recognition depends progressively on AI strategies, which use factual based measurements to isolate vindictive (secretive) traffic streams from the genuine (plain) ones. In any case, given the endeavors of digital assaults to dodge identification and the developing segment of CTC, incognito channels discovery needs to work on in both execution and accuracy to distinguish and forestall CTCs and relieve the decrease of the nature of administration brought about by the recognition cycle. In this paper, we present an inventive picture based answer for completely robotized CTC location and restriction.Our methodology depends on the perception that the secretive channels create traffic that can be changed over to shaded pictures. Utilizing this perception, our answer is intended to naturally recognize and find the malignant part (i.e., set of parcels) inside a traffic stream. By finding the incognito parts inside traffic streams, our methodology decreases the drop of the nature of administration brought about by hindering the whole traffic streams in which secret channels are distinguished. We first proselyte traffic streams into shaded pictures, and afterward we extricate picture based highlights for discovery undercover traffic. We train a classifier utilizing these elements on a huge informational index of undercover and clear traffic. This methodology shows an amazing exhibition accomplishing a recognition precision of 95.83% for wary CTCs and a secret traffic exactness of 97.83% for 8 cycle clandestine messages, which is far past what the famous measurable based arrangements can accomplish.**

Keywords: Covert Timing Channels,Elliptic-bend cryptography,Image Processing , Machine Learning

I. INTRODUCTION

Secretive channels give powerful strategies to exfiltrate touchy information from the designated networks. This kind of exfiltration is especially successful in light of the fact that it utilizes existing framework assets, which were not initially intended to send touchy information with the end goal of correspondence. By doing this, the exchange of the secret information becomes imperceptible by conventional location techniques, for example, firewalls and interruption discovery frameworks. Because of the capacity to send information without being identified, clandestine channels have turned into a genuine danger to the expert space just as the overall local area of web clients. Notwithstanding the way that undercover

channels can be utilized to release private data, they can be used by vindictive gatherings to convey and trade data to organize destroying Distributed Denial of Service (DDoS) assaults

II. LITERATURE SURVEY

Getting through the different measurements is unimaginable in the current framework. Encrypting the picture and getting the message at a similar time is preposterous. We talk about CTC location and anticipation approaches existing in the writing. The exploration works that we have considered for the plan and assessment of our proposed approach can be assembled into two principal classes: measurable based CTC discovery, and AI based CTC identification Poor association in the arrangement association.

CTC recognition strategies are for the most part centered around the investigation of organization traffic. Most CTC recognition strategies notice network traffic conduct and concentrate measurable properties of undercover and plain traffic and contrast those properties with perceived inconsistencies and identify clandestine correspondence .Similarly, in a parallel CTC was distinguished utilizing unmistakable traffic and secret traffic histogram. They examined a straightforward measurable strategy for distinguishing CTCs. This technique expects that a surge of organization traffic generally fits an ordinary circulation; a stream with a bimodal or multi-modular appropriation would propose the presence of a secretive planning channel. Consequently, the technique was among quick to zero in on anomalies looking like organization traffic dispersion. In their methodology, the choice tree was prepared utilizing different measurable elements removed from traffic streams. The model's adequacy in identifying the example of between appearance seasons of CTC parcels was then tried utilizing a bunch of both obvious and incognito traffic. The assessment consequences of this work showed that the model was compelling in recognizing CTCs.

[1] Shorouq Al-Eidi, Omar Darwishet al.,has proposed.In this paper Covert planning channels are a significant option for sending data in the realm of the Internet of Things (IoT). In clandestine planning, information is encoded in between appearance times between back to back bundles dependent on changing the transmission season of the real traffic. Commonly, the change of time happens by deferring the sent parcels on the sender side. A vital perspective in incognito planning channels is to observe the limit of parcel defer that can precisely recognize secretive traffic from genuine traffic. In light of that we can survey the degree of risk of safety dangers or the nature of moving delicate data subtly. In this paper, we concentrate on the between appearance time conduct of clandestine planning directed in two distinctive organization setups dependent on factual measurements, furthermore we explore the parcel postponing limit esteem. Our trials show that the limit is around equivalent to or more noteworthy than twofold the mean of authenticity between appearance times. For this situation secret planning channels become discernible as solid oddities.

This review utilized secret planning channels by altering the hour of genuine traffic and infusing the traffic that holds clandestine data inside the real traffic. The between appearance seasons of real traffic and secret traffic were examined in two diverse organization setups to investigate the conduct for the two deals with the two arrangements and see how the organization conditions impacted on the chomp rate transmission of the incognito planning channels and the exactness of recognizing clandestine traffic from genuine traffic. Our outcomes observed that the secret traffic didn't for the most part show outrageous qualities when the limit of parcel defers that used to conceal the undercover information was not exactly or equivalent the quarter of the mean of the between appearance seasons of real traffic. Thus, more incognito traffic is

counted near the real traffic, making the time scope of secretive traffic overlaps with the time scope of authentic traffic and the differentiation between them is hard. Notwithstanding, there is no crossover between the time scopes of [1]secretive traffic and the time scope of genuine traffic when the limit of parcel defers that is approximately equivalent to or more prominent than the twofold the mean between appearance seasons of authentic traffic, making the recognizing them more straightforward. In light of these perceptions, it is valuable to find these limits that can assist with recognizing the incognito from authentic traffic.

[2] Omar Darwish ,Ala Al-Fuqahaet al.,has proposed.In this paper Covert planning channels give a component to spill information across various substances. Controlling the circumstance between bundle appearances is a notable illustration of such methodology. The time based property makes the recognition of the secret messages inconceivable by conventional security ensuring instruments like intermediaries and firewalls. This paper presents another conventional various leveled based model to recognize secret planning channels. The location interaction comprises the examination of a bunch of factual measurements at continuous progressive levels of the between appearance times streams. The factual measurements considered are: mean, middle, standard deviation, entropy, Root of Average Mean Error (RAME). A genuinely factual measurements timing channel dataset of secret and plain channel occurrences is made. The produced dataset is set to be either level where the factual measurements are determined on all progressions of information or hierarchical (5 degrees of order were thought of) where the factual measurements are processed on sub pieces of the stream also. Following this technique, 5 unique datasets were created, and used to prepare/test a profound neural organization based model. Execution results about exactness and model preparing time showed that the various leveled approach outflanks the level one by 4 to 10 percent (as far as precision) and had the option to accomplish short model preparing time (as far as seconds).In our future work, we at first propose further expanding our model by broadening the current dataset with more issue space, measurable, and data hypothesis related elements. For the area related highlights, we will think about two expansive classes of elements: Hardware related (like CPU, switches, network speed, and so on); and Software related (kind of uses, sort of organization traffic, and so on) For the Statistical highlights, we will consider a subset of the measurements utilized in [2017] that incorporate mode, auto-connection coefficient, and so on With respect to data hypothesis related elements, we will consider extra measures, for example, Gini list to gauge the disparity (i.e., scattering) among between appearance times and Kullback-Leiber dissimilarity to remember data for how unique between appearance time disseminations act. Then, at that point, we will consider various sorts of convention epitomes, for example, UDP and crude attachments which don't initiate a great deal of buffering delays as the TCP convention does. At last, we will explore and execute new alleviation strategies as countermeasures against the distinguished incognito planning channels. We are likewise considering expanding our dataset by considering extra non-measurable highlights fully intent on further developing the clandestine planning channel recognition rate.

[3]Zhihua Cui, FeiXue,et al.,has proposed.In this paper With the advancement of the Internet, malevolent code assaults have expanded dramatically, with pernicious code variations positioning as a critical danger to Internet security. The capacity to recognize variations of vindictive code is basic for insurance against security breaks, information robbery, and different risks. Current techniques for perceiving vindictive code have shown helpless discovery precision and low location speeds. This paper proposed a clever strategy that pre-owned profound figuring out how to work on the recognition of malware variations. In earlier exploration, profound learning showed fantastic execution in picture acknowledgment. To carry out our proposed recognition strategy, we changed over the vindictive code into grayscale

pictures. Then, at that point, the pictures were recognized and ordered utilizing a convolutional neural organization (CNN) that could extricate the highlights of the malware pictures naturally. Furthermore, we used a bat calculation to address the information awkwardness among various malware families. To test our methodology, we led a progression of trials on malware picture information from Vision Research Lab. The test results showed that our model accomplished great exactness and speed as contrasted and other malware recognition models.This paper proposed a clever technique to work on the recognition of malware variations through the use of profound learning. To start with, this technique changed the vindictive code into grayscale pictures.

[4]Omar Darwish, Ala Al-Fuqahaet al.,has proposed.In this paper Leaking information utilizing clandestine planning channels is considered as a basic danger in network correspondence. These sort of channels utilize the time between appearance parcels to pass data between various cycles, making it extremely basic to plan procedures to wipe out and alleviate such channels; thus, guaranteeing a safer correspondence climate. This paper proposes another web based streaming way to deal with the relief of undercover planning channels. The new methodology disposes of undercover planning channels while little affecting the general Quality of Service (QoS). A classification based technique was utilized to test the exhibition of the proposed relief model. Clandestine planning channels are considered as quite possibly the most challenging dangers for spilling datum. The significance of concentrating on such sorts of channels ascended widely and quickly due to the limits of customary procedures (like intermediaries and firewalls) in recognizing these oddities and in the end reveal such dangers.

[5]Selim S. Sarikanet al.,has proposed.In this paper Anomaly identification is a significant piece of an Intelligent Transportation System. In this review, picture handling and AI procedures are utilized to distinguish irregularities in vehicle developments. These peculiarities remember standing and going for turn around bearing. Pictures are taken utilizing CCTV cameras from the front and back side of the vehicle. This capacity makes the outcomes strong to the varieties in functional and natural conditions. Various back to back outlines are gained for movement discovery. Elements, for example, edges and tag corner areas are separated for following purposes. Bearing of the traffic stream is acquired from the prepared classifier. K-closest neighbor is picked as the classifier model. The proposed strategy is assessed on a public parkway and promising identification results are accomplished. Abnormality discovery is such a significant issue that numerous Intelligent Transportation Systems (ITS) are looking into it. Distinguishing peculiarities in vehicles heading of development is a subset of this intricate issue. Vehicles moving off course represent a significant danger for different drivers. Without question, if peculiarities in vehicles bearing development are distinguished precisely continuously; hazard of mishaps can be diminished fundamentally. As the urban areas and transportation framework advance around more brilliant and more astute partners, observation frameworks become a fundamental issue.In this review, a vehicle stream identification way to deal with recognizing traffic oddities is introduced.

III.PROPOSED SYSTEM

Elliptical Curve Cryptography With Covert Timing Channels are utilized as the proposed technique Machine learning calculations have been utilized in numerous CTC location approaches in view of their capacity to successfully recognize secretive planning channels. As a rule, these methodologies utilize different measurements (or elements) to prepare and develop AI models utilizing a marked arrangement of obvious and incognito traffic streams. a clever procedure for computerized and exact identification of secret planning channels. Defeated exhaustively and got to the picture encryption.

Circular bend cryptography with undercover planning channels are exceptionally effective and less tedious. Elliptic-bend cryptography (ECC) is a way to deal with public key cryptography dependent on the logarithmic construction of elliptic bends over limited fields. ECC permits more modest keys contrasted with non-ECC cryptography (in light of plain Galois fields) to give the same. In PC security, an incognito channel is a sort of assault that makes a capacity to move data objects between processes that shouldn't be permitted to convey by the PC security strategy Security.

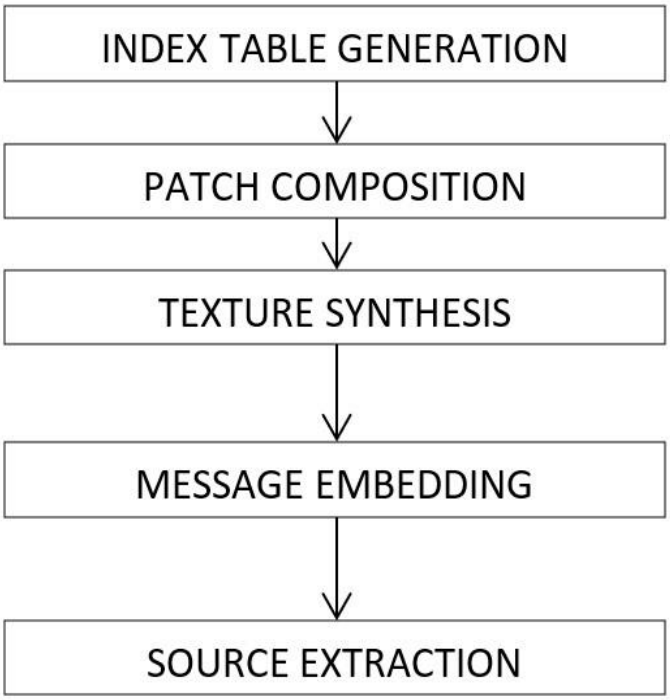

Fig 1 : Architecture Design

IV. METHODOLOGY

INDEX TABLE GENERATION

In the file esteem age the finished picture is stacked and the worth is given with the specific spot as indicated by the surface of the picture pixels.

This can be utilized to store the message and scramble the information and recover the data

TEXTURE SYNTHESIS

A fix is a bunch of changes to a PC program or its supporting information intended to refresh, fix, or further develop it. This incorporates fixing security weaknesses and different bugs, with such fixes normally being called bug fixes or bug fixes.

Fixing makes conceivable the alteration of aggregated and picture object programs when the source code is inaccessible.

This requests a careful comprehension of the inward functions of the article code by the individual making the fix, which is troublesome without close investigation of the source code.

PATCH COMPOSITION

Surface Synthesis is the course of algorithmically developing an enormous computerized picture from a little advanced example picture by exploiting its underlying substance.

It is an object of exploration in PC designs and is utilized in many fields, among steganography

MESSAGE EMBEDDING

The information stowed away will essentially be equivalent to the rest by partitioning the new pixel by likewise.

This is a technique where the information is concealed in the contrast between the nearby pixels, so simple extraction of a few pieces won't ever give the information stowed away.

MACHINE LEARNING MODEL CONSTRUCTION

Our methodology's last advance is to develop an AI model to group the produced pictures into one or the other clandestine or obvious. For this assignment, we train a bunch of models utilizing the following AI calculations:

Support Vector Machine (SVM).

V.RESULTS AND DISCUSSION

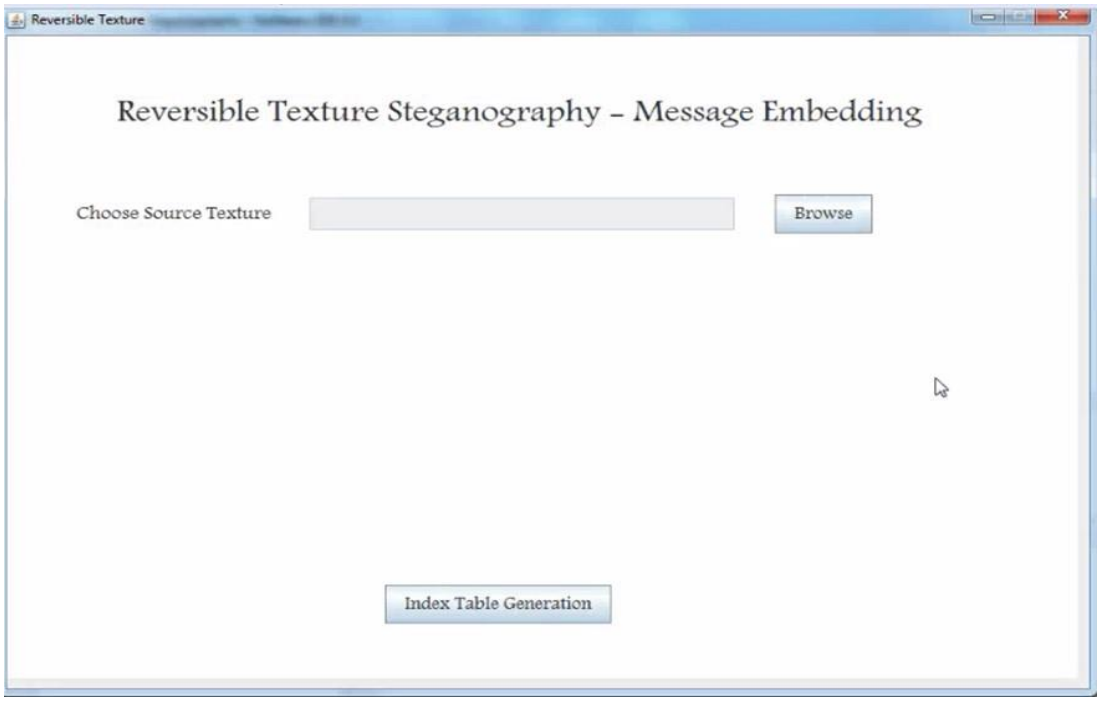

Fig 2 : Reversible Texture Steganography

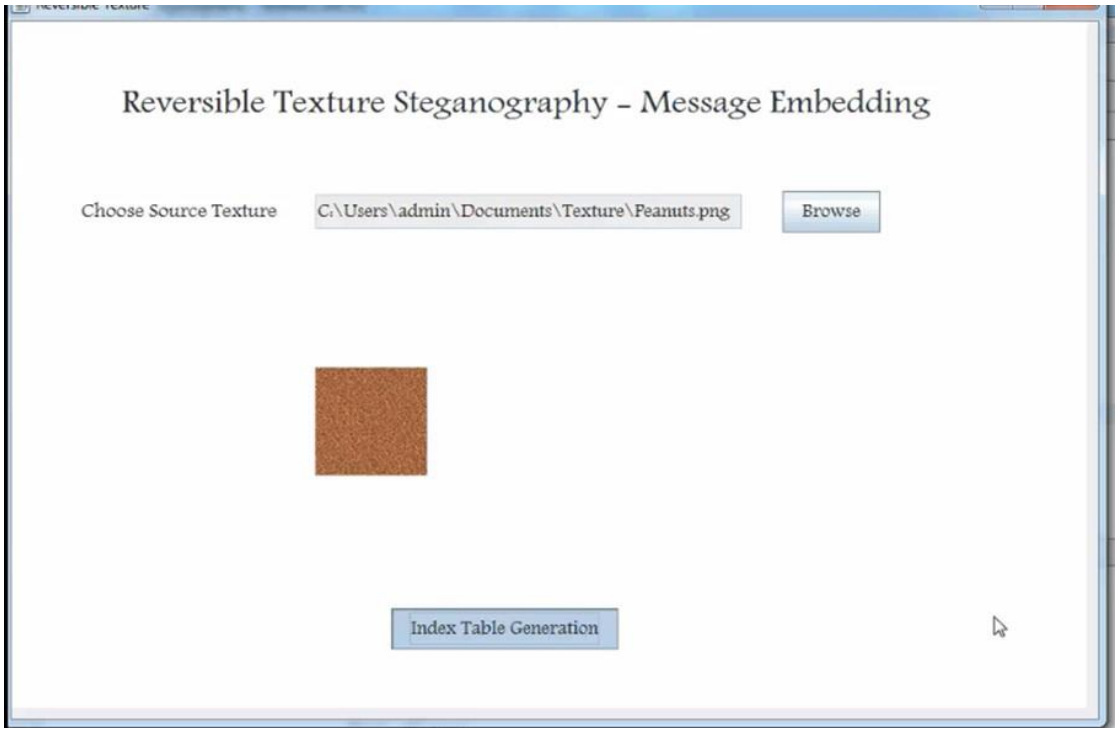

Fig 3 : Message Embedding

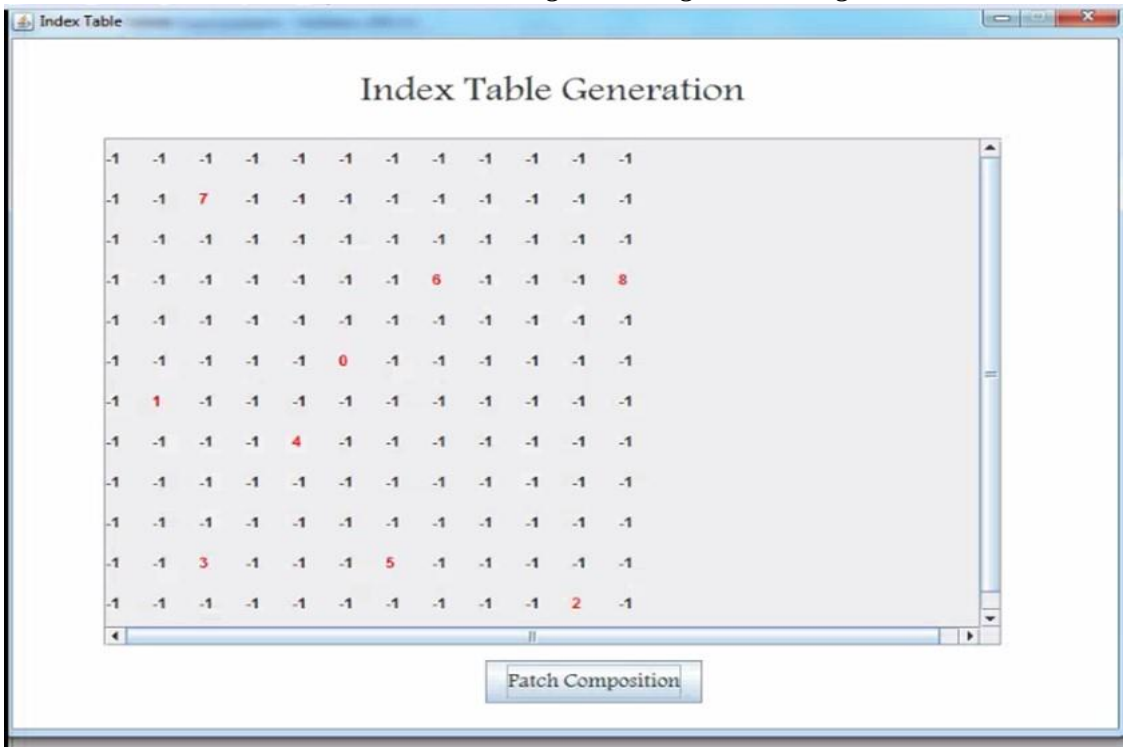

Fig 4 : Index Table Generation

VI. CONCLUSION AND FUTURE SCOPE

We present Snap Catch, an original strategy for mechanize and precise discovery of clandestine planning stations. Snap Catch is intended to practice picture handling and AI methods for secret traffic location. To begin with, the framework changes over the between appearance seasons of traffic into hued pictures utilizing an inventive instrument that catches the substantial highlights of organization traffic and addresses them in hued pictures. By extricating strong and precise highlights from the shaded pictures, Snap Catch trains different AI classifiers to proficiently identify secretive channels dependent on a tunable protection system that focuses on (or balances) exactness and fulfillment. What's more, we propose a component to pinpoint the secret messages (i.e., set of parcels) inside a traffic stream to permit dropping just a portion of the traffic stream that contains the clandestine message rather than the whole stream.

Our assessment of Snap Catch shows that it beats the adjusted contingent entropy, entropy, and routineness approaches. Further, our methodology shows the least presentation misfortune in distinguishing little undercover messages and the super-weak clandestine channels (UCCTC), the most developed kind of secret digital assaults. Snap Catch endlessly beats the gauge approaches in distinguishing the portions inside traffic streams that convey clandestine messages, which altogether decreases the deficiency of the nature of administration brought about by dropping incognito traffic streams. At long last, we give different situations and use cases for tuning Snap Catch to execute a guard methodology that fits the instrument clients' assets and security goals.

VII. REFERENCES

[1] S. Valarmathy, R. Ramani, Fahim Akhtar, S. Selvaraju, G. Ramachandran, “Automatic Ration Material Distributions based on GSM and RFID Technology”, I. J Intelligent System and Applications(ijisa) S. Al-Eidi, O. Darwish, and Y. Chen. Covert timing channel analysis either as cyber attacks or confidential applications. Sensors, 20(8):2417, 2020.

[2] B. Anderson, C. Storlie, and T. Lane. Improving malware classification: bridging the static/dynamic gap. In Proceedings of the 5th ACM workshop on Security and artificial intelligence, pages 3–14, 2012.

[3] R. Archibald and D. Ghosal. A comparative analysis of detection metrics for covert timing channels. Computers & security, 45:284–292, 2014.

[4] A. Askarov, D. Zhang, and A. C. Myers. Predictive black-box mitigation of timing channels. In Proceedings of the 17th ACM conference on Computer and communications security, pages 297–307, 2010.

[5] V. Berk, A. Giani, G. Cybenko, and N. Hanover. Detection of covert channel encoding in network packet delays. Rapport technique TR536, de lUniversité de Dartmouth, 19, 2005.

[6] A. K. Biswas, D. Ghosal, and S. Nagaraja. A survey of timing channels and countermeasures. ACM Computing Surveys (CSUR), 50(1):1–39, 2017.

[7] K. Borders and A. Prakash. Web tap: detecting covert web traffic. In Pro- ceedings of the 11th ACM conference on Computer and communications security, pages 110–120, 2004.

[8] S. Cabuk. Network covert channels: Design, analysis, detection, and elimination. PhD thesis, Purdue University, 2006.

[9] S. Cabuk, C. E. Brodley, and C. Shields. Ip covert timing channels: design and detection. In Proceedings of the 11th ACM conference on Computer and communications security, pages 178–187. ACM, 2004.

[10] L. Chappell. Wireshark 101: Essential skills for network analysis- wireshark solution series. Laura Chappell University, USA, 2017.

[11] Z. Cui, F. Xue, X. Cai, Y. Cao, G.-g. Wang, and J. Chen. Detection of malicious code variants based on deep learning. IEEE Transactions on Industrial Informatics, 14(7):3187–3196, 2018.

[12] O. Darwish, A. Al-Fuqaha, M. Anan, and N. Nasser. The role of hierarchi- cal entropy analysis in the detection and time-scale determination of covert timing channels. In 2015 International Wireless Communications and Mobile Computing Conference (IWCMC), pages 153–159. IEEE, 2015.

[13] O. Darwish, A. Al-Fuqaha, G. B. Brahim, and M. A. Javed. Using mapre- duce and hierarchical entropy analysis to speed-up the detection of covert timing channels. In 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), pages 1102–1107. IEEE, 2017.

[14] O. Darwish, A. Al-Fuqaha, G. B. Brahim, I. Jenhani, and M. Anan. To- wards a streaming approach to the mitigation of covert timing channels. In 2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC), pages 255–260. IEEE, 2018.

[15] O. Darwish, A. Al-Fuqaha, G. B. Brahim, I. Jenhani, and A. Vasilakos. Using hierarchical statistical analysis and deep neural networks to detect covert timing channels. Applied Soft Computing, 82:105546, 2019. [16] K. Denney, A. S. Uluagac, K. Akkaya, and S. Bhansali. A novel storage covert channel on wearable devices using status bar notifications. In 2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC), pages 845–848. IEEE, 2016.

[16] S. Zander, G. Armitage, and P. Branch. Stealthier inter-packet timing covert channels. In the International Conference on Research in Networking, pages 458–470. Springer, 2011.

[17] S. Gianvecchio and H. Wang. An entropy-based approach to detecting covert timing channels. IEEE Transactions on Dependable and Secure Computing, 8(6):785–797, 2010.

[18] S. Gianvecchio and H. Wang. An entropy-based approach to detecting covert timing channels. IEEE Transactions on Dependable and Secure Computing, 8(6):785–797, 2010.

[19] S. Gianvecchio, H. Wang, D. Wijesekera, and S. Jajodia. Model-based covert timing channels: Automated modeling and evasion. In International Workshop on Recent Advances in Intrusion Detection, pages 211–230. Springer, 2008.

[20] M. Hall, E. Frank, G. Holmes, B. Pfahringer, P. Reutemann, and I. H. Witten. The weka data mining software: an update. ACM SIGKDD explorations newsletter, 11(1):10–18, 2009.

[21] K. Han, J. H. Lim, and E. G. Im. Malware analysis method using visualization of binary files. In Proceedings of the 2013 Research in Adaptive and Convergent Systems, pages 317–321. 2013.

[22] J. D. Hunter. Matplotlib: A 2d graphics environment. Computing in science & engineering, 9(3):90–95, 2007.

[23] F. Iglesias, R. Annessi, and T. Zseby. Dat detectors: uncovering tcp/ip covert channels by descriptive analytics. Security and Communication Networks, 9(15):3011–3029, 2016.

[24] F. Iglesias, V. Bernhardt, R. Annessi, and T. Zseby. Decision tree rule induction for detecting covert timing channels in tcp/ip traffic. In Inter- national Cross-Domain Conference for Machine Learning and Knowledge Extraction, pages 105–122. Springer, 2017.

[25] F. Iglesias and T. Zseby. Are network covert timing channels statistical anomalies? In Proceedings of the 12th International Conference on Availability, Reliability and Security, pages 1–9, 2017.

[26] M. H. Kang, I. S. Moskowitz, and S. Chincheck. The pump: A decade of covert fun. In 21st Annual Computer Security Applications Conference (ACSAC 05), pages 7–pp. IEEE, 2005.

[27] S. S. Kim and A. N. Reddy. Modeling network traffic as images. In IEEE International Conference on Communications, 2005. ICC 2005. 2005, volume 1, pages 168–172. IEEE, 2005.

[28] S. S. Kim and A. N. Reddy. A study of analyzing network traffic as images in real-time. In Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies., volume 3, pages 2056– 2067. IEEE, 2005.

[29] N. Kiyavash, F. Koushanfar, T. P. Coleman, and M. Rodrigues. timing channel spyware for the csma/ca protocol. IEEE Transactions on Information Forensics and Security, 8(3):477–487, 2013.

[30] X. Liu, Y. Sun, L. Fang, J. Liu, and L. Yu. A survey of network traffic visualization in detecting network security threats. In International Con- ference on Trustworthy Computing and Services, pages 91–98. Springer, 2014.

[31] Y. Liu, D. Ghosal, F. Armknecht, A.-R. Sadeghi, S. Schulz, and S. Katzen- beisser. Hide and seek in time—robust covert timing channels. In the European Symposium on Research in Computer Security, pages 120–135. Springer, 2009.

[32] J.-S. Luo and D. C.-T. Lo. Binary malware image classification using machine learning with local binary pattern. In 2017 IEEE International Conference on Big Data (Big Data), pages 4664–4667. IEEE, 2017. [33] X. Ma, Z. Dai, Z. He, J. Ma, Y. Wang, and Y. Wang. Learning traffic as images: a deep convolutional neural network for large-scale transportation network speed prediction. Sensors, 17(4):818, 2017.

[34] A. Makandar and A. Patriot. Malware analysis and classification using artificial neural networks. In 2015 International conference on trends in automation, communications and computing technology (I-TACT-15), pages 1–6. IEEE, 2015.

[35] A. Makandar and A. Patriot. Wavelet statistical feature based malware class recognition and classification using supervised learning classifier. Oriental journal of computer science and technology, 10(2):400–406, 2017. [36] M. Mehic, J. Slachta, and M. Voznak. Whispering through ddos attack. Perspectives in Science, 7:95–100, 2016.

[37] S. Mou, Z. Zhao, S. Jiang, Z. Wu, and J. Zhu. Feature extraction and classification algorithm for detecting complex covert timing channels. Computers & Security, 31(1):70–82, 2012.

[38] H. Najadat, Y. Jaffal, O. Darwish, and N. Yasser. A classifier to detect abnormality in ct brain images. In Proceedings of the International Multi- conference of Engineers and Computer Scientists, pages 16–18.

Citeseer, 2011.

[39] L. Nataraj, S. Karthikeyan, G. Jacob, and B. Manjunath. Malware images: visualization and automatic classification. In Proceedings of the 8th international symposium on visualization for cyber security, pages 1–7, 2011.

[40] R. Paul, S. H. Hawkins, L. O. Hall, D. B. Goldgof, and R. J. Gillies. Combining deep neural network and traditional image features to improve survival prediction accuracy for lung cancer patients from diagnostic ct. In 2016 IEEE International Conference on Systems, Man, and Cybernetics (SMC), pages 002570–002575. IEEE, 2016.

[41] P. Peng, P. Ning, and D. S. Reeves.On the secrecy of timing-based active watermarking trace-back techniques. In 2006 IEEE Symposium on Security and Privacy (S&P'06), pages 15–pp. IEEE, 2006.

[42] W. Rasband. 1997–2018 image. Bethesda, MD: US National Institutes of Health.

[43] S. S. Sarikan and A. M. Ozbayoglu. Anomaly detection in vehicle traffic with image processing and machine learning. Procedia Computer Science, 140:64–69, 2018.

[44] P. L. Shrestha, M. Hempel, F. Rezaei, and H. Sharif. Leveraging statistical feature points for generalized detection of covert timing channels. In 2014 IEEE Military Communications Conference, pages 7–11. IEEE, 2014.

[45] P. L. Shrestha, M. Hempel, F. Rezaei, and H. Sharif. A support vector machine-based framework for detection of covert timing channels. IEEE Transactions on Dependable and Secure Computing, 13(2):274–283, 2015.

[46] T. Sohn, J. Moon, S. Lee, D. H. Lee, and J. Lim. Covert channel detection in the icmp payload using a support vector machine. In International Sym- posium on Computer and Information Sciences, pages 828–835. Springer, 2003.

[47] T. H. A. Soliman, R. Mohamed, and A. A. Sewissy. A hybrid analytical hierarchical process and deep neural networks approach for classifying breast cancer. In 2016 11th International Conference on Computer Engineering & Systems (ICCES), pages 212–219. IEEE, 2016.